International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 16th Aug 2017. Link :http://www.ijiemr.org/downloads.php?vol=Volume-6&issue=ISSUE-7

Title: **An Adaptive Digital Image Forgery Detection Model With Copy Move Operations Based On Block Feature Matching Algorithm And Forgery Region Extraction Algorithm**

Volume 06, Issue 07, Pages: 1 – 10.

Paper Authors

VIJAY SHANKER NALLAPATI [1], DR GIRISH CHANDRA[2]

* University of Allahabad, Allahabad, U.P India

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

AN ADAPTIVE DIGITAL IMAGE FORGERY DETECTION MODEL WITH COPY MOVE OPERATIONS BASED ON BLOCK FEATURE MATCHING ALGORITHM AND FORGERY REGION EXTRACTION ALGORITHM

VIJAY SHANKER NALLAPATI [1], **DR GIRISH CHANDRA**[2]

[1]Research Scholar, Department of Electronics and Communication Engineering, University of Allahabad, Allahabad, U.P India

[2]Professor, Department of Electronics and Communication Engineering, University of Allahabad, Allahabad, U.P India

Abstract---The digital images have been widely used for various purposes such as segmentation, compression, enhancement, classification, detection, etc., in different modern applications such as navigation, medical analysis, satellite imagery, marine science and so on. The digital images are widely used to maintain confidentiality and to protect the authentication of the user credibility in well defined manner. The challenging issue frequently facing in the 21st century is the image duplicity which is also called as the image forgery, although it start's as the fun for Photoshop the images but rises to utmost level in negative side which poses serious challenges to researchers to develop new algorithms to detect the forged content in the original image. The copy-move operations has make use of the image overlay operations to introduce the forged content in the original image and its detection remains challenging task in the field of the digital image processing. An adaptive over segmentation algorithm in collaboration with the Block Feature Matching Algorithm and Forgery Region Extraction Algorithm has created a excellent solution to detect the forged elements in the image and the usage of the super pixels make way for the user friendly segmentation in simple way. The experimental results shows the proposed methodology performance in terms of the precision, F-measure and the recall, when compare with existing state of art methods the proposed methodology achieves good accuracy with minimal time consumption.

Index Terms: Digital image processing, Image forgery, Copy-move operations, Adaptive over segmentation, Matching algorithm, Extraction algorithm, Forgery detection.

1. INTRODUCTION

The digital images are consider as the primary choice for the information in all major modern world applications and the introduction of the digital image forgery concept has totally put a question mark (doubt) on the image credibility and the its reliability. The digital image forgery has created as serious buzz in the world of the digital image processing and the situation force the researchers to find the appropriate solution to restore the faith in the image information with good reliability. A lot of research work is carried out in the past years to detect the accurate image forgery detection algorithms and to find the ways that how a image is made forged, the research has revealed the mind blowing facts that the image overlay and the copy move operations are the major way to introduce the forged elements in the original image. The copy-move operation is basically copying the noise component, color content and the other image processing properties. The concept of the image forgery and the image tampering is active research area for over the decade and the issue has raised many questions on the credibility of the image information and made it more doubtful. The intense research is carried out by world's famous and renowned research organizations under qualified researchers. The common practice followed to introduce the forged elements in the image s copying single or multiple copied regions in the original image at different locations and this operation is technically called as copy-move operations in the image processing terminology. The copy-move process is involved with variety of image processing operations such as rotation, scaling, blurring, compression, and noise addition. The mentioned image processing operations is applied to make the original image elements with forged elements with perfection. The implementation of the wide range of the image forgery detection algorithms are developed but none can meet the practical requirements.The integrity of the digital images and its validation is a concerned area from past two decades from the date of the image forgery came into existence. The popular research fields such as medical imaging and its statistics, online shopping, forensics, high quality professional photography needs the authenticity and the reliability to trust the information a digital image can posses. The medical imaging is related human life and the physician's suggest the treatment based on the images which they perceive, if they have forged images then it costs the human life. With professionals challenging the ethical boundaries of truth, it creates a potential loss of public trust in digital media. This motivates the need for detection tools that are transparent to tampering and can tell whether an image has been tampered just by inspecting the tampered image. Image tampering is a digital art which needs understanding of image properties and good visual creativity. One tampers images for various reasons either to enjoy fun of digital works creating incredible photos or to produce false evidence. No matter whatever the cause of act might be, the forger should use a single or a combination series of image processing operations.

2. LITERATURE REVIEW

2.1 Detecting Duplicated Image

Alin C Popescu et al.(2004) proposed a technique that works by first applying principal component analysis to small fixed-size image blocks to yield a reduced dimension representation. Duplicated regions are then detected by lexicographically sorting all of the image blocks. This technique is effective on plausible forgeries, and have quantified its sensitivity to JPEG lossy compression and additive noise. Detection is possible even in the presence of significant amounts of corrupting noise using this method.

2.2 Fast Copy-Move Forgery Detection

Hwei-jen lin et.al (2009) have proposed a method to detect copy- move forgery by dividing the image into overlapping blocks of equal size, extracting feature for each block and representing it as a vector and sorting all the extracted feature vectors using the radix sort. Radix sort dramatically reduces the time complexity and the adopted features enhance the capability of resisting of various attacks such as JPEG compression and Gaussian noise. Both efficiency and high detection rates have been demonstrated. A few small copied regions were not successfully detected. Although duplicated regions with rotation through some fixed angles can be detected, this method does not deal with rotation arbitrary angles.

2.3 Robust Copy-move Forgery

Sevinc Bayram et al.(2009) proposed to use Fourier-Mellin Transform (FMT) features which are invariant to scaling and translation. They also presented a new detection scheme that make use of counting bloom filters. It detects copymove forgery very accurately even if the forged image is rotated, scaled or highly compressed. This detection scheme improves the efficiency, but the robustness of the method is reduced.

2.4 Fast and Robust Image Region

WANG Jun-Wen et.al. (2009) proposed an algorithm to detect region-duplication forgery where the image is first reduced in dimension by Gaussian pyramid, and the Hu moment is applied to the fixed sized overlapping blocks of low-frequency image. The eigenvectors are lexicographically sorted. Then, similar eigenvectors are matched by a certain threshold value. Finally, the area threshold value is proposed to remove the wrong similar blocks. This method is robust and it can not only successfully detect this type of tampering for images subject to various forms of post region duplication image processing, including noise contamination, blurring, and severe lossy compression, but also reduce the total number of blocks to narrow block-matching searching space, which can improve the method efficiency. The detection rate of this method is low and also it works only within same image and does not work between different images.

2.5 Region detection Using Image Feature Matching

Xunyu Pan et al. (2010) proposed a method for region duplication detection by estimating the transform between matched SIFT keypoints and then finding the duplicated regions after discounting the estimated transforms. It is effective even when the duplicated regions are distorted. SIFT algorithm cannot find the reliable keypoints in regions with little visual structures. Also, smaller regions having fewer keypoints hard to detect. Images having intrinsically identical regions cannot be differentiated from intentionally duplicated regions.

3. EXISTING METHOD

Traditional system used block based forgery detection and feature matching algorithm separately .In previous years, many forgery detection methods have been proposed for copy-move forgery detection. According to the existing methods, the copy-move forgery detection method scan be categorized into two main categories: block-based algorithms and feature key point-based algorithms. The existing block-based forgery detection methods divide the input images into overlapping and regular image blocks; then, the tampered region can be obtained by matching blocks of image pixels or transform coefficients.Most of the existing block-based forgery detection algorithms use a similar framework, and the only difference is that they apply different feature extraction methods to extract the block features.Although the existing keypoint-based forgery detection methods can avoid computational complexity and can successfully detect the forgery, even when some attacks exist in the host images; the recall results of the existing keypoint-based forgery methods were very poor.From which the quantized Discrete Cosine Transform (DCT) coefficients of the blocks were matched to find the tampered regions. Popescu and Farid applied Principal Component Analysis (PCA) to reduce the feature dimensions.Luoet al. [used the RGB color components and direction information as block features. Li et al. Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) to extract the image features. Mahdian and Saic calculated the 24 Blur-invariant moments as features. Kang and Wei calculated the singular values of a reduced-rank approximation in each block. Bayram et al. used the Fourier-Mellin Transform (FMT) to obtain features. Wang et al. The mean intensities of circles with different radii around the block center to represent the block features.Lin et al. used the gray average results of each block and its sub-blocks as the block features. Ryu et al. Zernike moments as block features. Bravo-Solorio and Nandi used information entropy as block features. As an alternative to the block-based methods, key point based forgery detection methods were proposed, where image key points are extracted and matched over the whole image to resist some image transformation while identifying duplicated regions. In Scale-Invariant Feature Transform (SIFT) was applied to the host images to extract feature points, which were then matched to one another. When the value of the shift vector exceeded the threshold, the sets of corresponding SIFT feature points were defined as the forgery region.However, although these methods can locate the matched key points, most of them cannot locate the forgery regions very well; therefore, they cannot achieve satisfactory detection results and, at the same time, a sustained high recall rate . Most of the existing block-based forgery detection algorithms use a similar framework, and the only difference is that they apply different feature extraction methods to extract the block features.

Disadvantages

- The host image is divided into over-lapping rectangular blocks, which would be computationally expensive as the size of the image increases.

- The method cannot address significant geometrical transformations of the forgery regions

- Their recall rate is low because their blocking method is regular shape.

4. PROPOSED METHODOLOGY

The proposed methodology and its dominance over the traditional methods lies in the integration of the traditional block based forgery detection approach and the key point based forgery detection methods. The secret of the proposed methodology lies in the adaptive over segmentation method which is primarily used to divide the original host image into the non–overlapping an irregular blocks in adaptive manner and the entire process is quite similar to the block based forgery detection. Unlike the traditional key point base method where the whole host image is used to extract the features, in proposed method key point features are extracted from the available blocks which helps to accomplish the task in mean time as previously decided. Finally the suspected forged elements and its regions are detected using the process of performing the matching between the features of each block with another and to get the forgery regions in accurate manner the algorithm named forgery region extraction is used in the proposed method. The forgery extraction algorithm is used to replace the feature points with the small super pixels as feature blocks and the entire process is merged with the morphological operations to generate the detected forged regions in well defined manner.

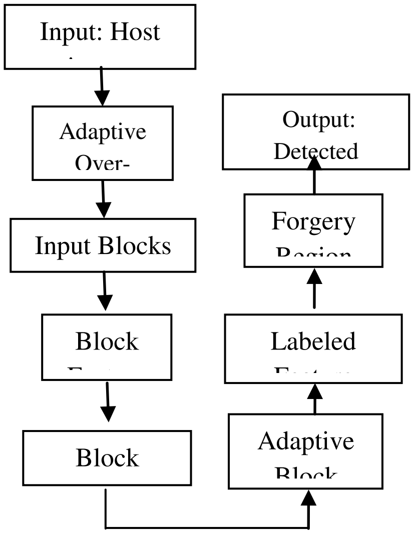

Fig. 1: The Proposed Copy-Move Forgery Detection Scheme

The proposed methodology is classified into three important steps as mentioned below fig. 2. The three different steps perform their own operation to extract the exact forged elements from the original image in the detection process.

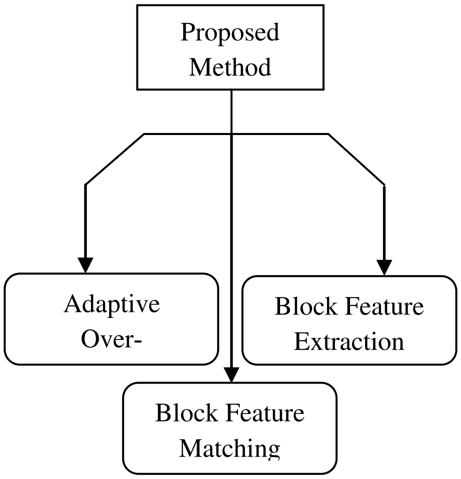

Fig. 2: The classification of the proposed Copy-Move Forgery Detection algorithms

(A) Adaptive over segmentation

- The purpose of the proposing the adaptive over segmentation algorithm is to reduce the cost while the existing methods have the matching computation at high cost and to tackle the issue the adaptive over segmentation is used.
- The host image is divided into non overlapping blocks
- The host image is divided into irregular shapes
- The forgery detection is done performing the matching between these non overlapping blocks and the irregular shapes
- The regular blocks fail in some cases to detect the forgery regions while the proposed adaptive segmentation method has the irregular blocks which never fail in the detection process.
- The SLIC approach is introduced which makes it difficult to decide the super pixels shape and the size.
- Unlike the traditional segmentation, the super pixels produce different sizes which help to produce the different forgery results in well defined manner
- Consequently, different host images should be blocked into super pixels of different initial sizes, which is highly related to the forgery detection results.

(B) Block Feature Extraction

- The block feature extraction has high importance in the proposed methodology and these block feature are extracted from the image blocks (IB).
- The traditional methods extract the features of same size which creates difficulty in assessing the information.
- However, these features reflect mainly the content of the image blocks, leaving out the location information. Also, these features are not resistant to various image transformations.
- Therefore, in this project, the feature points are extracted from each image

block as block features and the feature points should be robust to various distortions, such as image scaling, rotation, and JPEG compression.

- The feature points generated using these methods are robust against common image processing operations such as rotation, scale, blurring, and compression.
- Hence, in this project SIFT is used for feature point extraction. Therefore, each block feature contains irregular block region information and the extracted SIFT feature points.

(C) Block Feature Matching

- In most of the existing block-based methods, the block matching process outputs a specific block pair only if there are many other matching pairs in the same mutual position, assuming that they have the same shift vector.
- When the shift vector exceeds a user-specified threshold, the matched blocks that contributed to that specific shift vector are identified as regions that might have been copied and moved.
- In our algorithm, because the block feature is composed of a set of feature points, we proposed a different method to locate the matched blocks.

Algorithm: Forgery Region Extraction

- **STEP-1:** Load the Labeled Feature Points (LFP), apply the SLIC algorithm with the initial size S to the host image to segment it into small superpixels as feature blocks, and replace each labeled feature point with its corresponding feature block, thus generating the Suspected Regions (SR).
- **STEP-2:** Measure the local color feature of the superpixels neighbor to the SR, called neighbor blocks; when their color feature is similar to that of the suspected regions, we merge the neighbor blocks into the corresponding SR, therefore creating the merged regions (MR).
- **STEP-3:** Apply the morphological close operation into MR to finally generate the detected forgery regions.

5. RESULTS

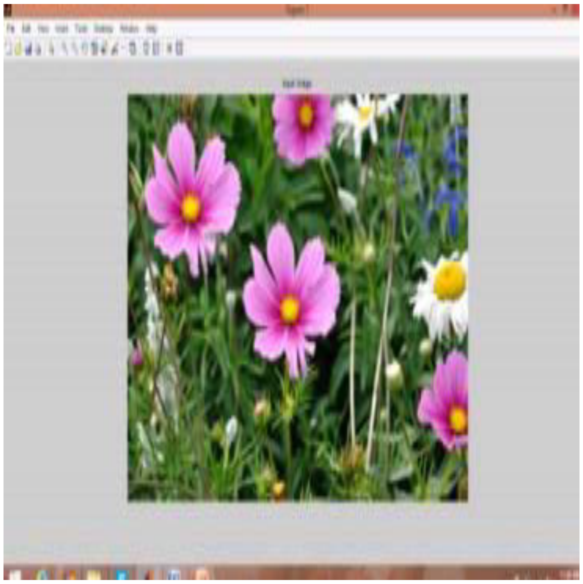

Fig. 3: Input image

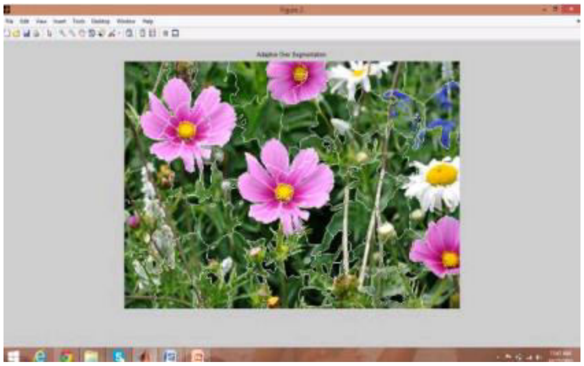

Fig. 4: Segmented by Adaptive overlap Image

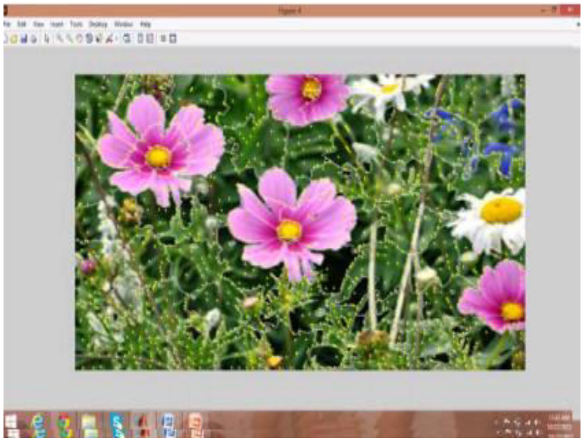

Fig. 5: Future Point Extraction

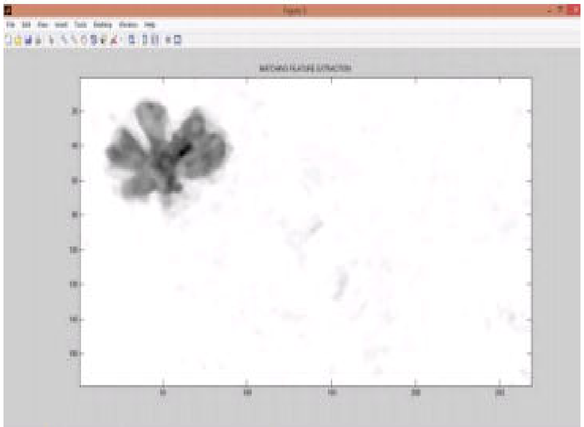

Fig. 6: Forgery Image

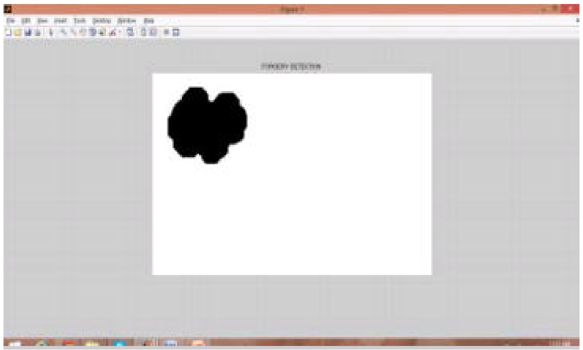

Fig. 7: Forgery Region

6. CONCLUSION

Digital forgery images created with copy-move operations are challenging to detect. In this paper, we have proposed a novel copy-move forgery detection scheme using adaptive over-segmentation and feature-point matching. The Adaptive Over Segmentation algorithm is proposed to segment the host image into non-overlapping and irregular blocks adaptively according to the given host images; using this approach, for each image, we can determine an appropriate block initial size to enhance the accuracy of the forgery detection results and, at the same time, reduce the computational expenses. Then, in each block, the feature points are extracted as block features, and the Block Feature Matching algorithm is proposed, with which the block features are matched with one another to locate the labeled feature points; this procedure can approximately indicate the suspected forgery regions. Subsequently, to detect the more accurate forgery regions, we propose the Forgery Region Extraction algorithm, in which the labeled feature points are replaced with small super pixels as feature blocks, and the neighboring feature blocks with local color features that are similar to the feature blocks are merged to generate the merged regions. Next, the morphological operation is applied to the merged regions to generate the detected forgery regions.

REFERENCES

[1] J. Fridrich, D. Soukal, and J. Lukáš , "Detection of copy–move forgery in digital images," in Proc. Digit. Forensic Res. Workshop, Cleveland, OH, Aug. 2003.

[2] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dept. Comput. Sci. NH, USA, Tech. Rep. TR2004-515, 2004.

[3] W. Luo, J. Huang,“ Detection of region-duplication of image,"Proc. 18th Pattern Recognit. (ICPR), Aug. 2006.

[4] G. Li, Q. Wu, D. Tu, and S. Sun, "A sorted neighborhood approach for detecting region , in Proc. IEEE Int. Conf. Multimedia Expo, Jul. 2007, pp. 1750–1753.

[5] B. Mahdian and S. Saic, "Detection of copy–move forgery using a method based on moment invariants," Forensic Sci. Int., vol. 171, nos. 2–3, pp. 180–189, 2007.

[6] X. B. Kang and S. M. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics," in Proc. Int. Dec. 2008, pp. 926–930.

[7] S. Bayram, H. T. Sencar,"An efficient and robust method for copy–move forgery," in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP), Apr. 2009, pp. 1053–1056.

[8] J. Wang, G. Liu, H. Li, Y. Dai, and Z. Wang, "Detection of image region duplication forgery using model with circle block," in Proc. Int. Conf. Multimedia Inf. Netw. Secur. (MINES), Nov. 2009, pp. 25–29.

[9] J. W. Wang, G. J. Liu, Z. Zhang, Y. W. Dai, and Z. Q. Wang, "Fast and robust forensics for image region-duplication forgery," Acta Automat. Sinica, vol. 35, no. 12,

[10] H. J. Lin, C. W. Wang, and Y. T. Kao, "Fast copy–move forgery detection," WSEAS Trans. Signal Process., vol. 5, no. 5, pp. 188–197, 2009.

[11] S. J. Ryu, M. J. Lee, and H. K. Lee, "Detection of copy-rotate-move forgery using Zernike moments," in Information Hiding. Berlin, Germany: Springer-Verlag, 2010, pp. 51–65.

[12] S. J. Ryu, M. Kirchner, M. J. Lee, and H. K. Lee, "Rotation invariant localization of duplicated image regions based on Zernike moments," Aug. 2013.

[13] S. Bravo-Solorio , "Exposing duplicated regions affected by reflection, and scaling," in Proc. IEEE Int. Conf.

Acoust., Speech, Signal Process. (ICASSP), May 2011, pp. 1880–1883.

[14] H. Huang, W. Guo, and Y. Zhang, "Detection of copy–move forgery in digital images using SIFT algorithm," in Proc. Pacific-Asia Workshop Comput. Intell. Ind. Appl. (PACIIA), Dec. 2008, pp. 272–276.

[15] X. Pan and S. Lyu, "Region duplication detection using image feature matching," IEEE Trans. Inf. Forensics Security, vol. 5, no. 4, pp. 857– 867, Dec. 2010.